



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/543,009

07/22/2005

Kazuya Oyama

2936-0245PUS1

1180

2292 7590 01/23/2009
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER

HAILU, TESHOME

ART UNIT

PAPER NUMBER

2439

NOTIFICATION DATE

DELIVERY MODE

01/23/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

| | | | |
|------------------------------|--------------------------------------|-------------------------------------|--|
| Office Action Summary | Application No. 10/543,009 | Applicant(s) OYAMA ET AL. | |
| | Examiner TESHOME HAILU | Art Unit 2439 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 November 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2439

DETAILED ACTION

1. This office action is in reply to an amendment filed on November 05, 2008. Claims 1-41 have been amended.
2. Claims 1-41 are pending.

Response to Amendment

3. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 21 and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim limitation, "a code management control portion that compares a plurality of the encryption codes received by the code management reception portion", is not clear to the examiner. Examiner understands that the limitation is comparing a plurality of encryption code with the stored encryption code. However, according to the claim limitation, it is not clear that the result of the comparison. The limitation is silent about the kind of comparison.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-7, 11-26 and 30-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al (Son) (US Pub. No. 2001/0017920) in view of Kim (US Pub. No. 2003/0164750).

As per claim 1 Son discloses:

An encryption code management system for use in a plurality of communication systems composed of a plurality of data processors that exchange data encrypted with specific encryption codes, (page 1, paragraph 3, the present invention relates to the field of secure video distribution networks).

Wherein there is provided an electronic apparatus including: a code management reception portion that receives the encryption codes of the data processors; (abstract, line 1-5, an encrypted form of video program received by the remote server and stored). The remote server is a distribution center acting as an intermediate device between the service provider and subscriber station.

Son does not explicitly disclose the system of receiving the encryption codes of the data processors. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 35, the security system according to the present invention is comprised of a receiving unit 20 for receiving the signal transmitted from the wireless communication system 10, a storage unit 30 for storing a specific information of the wireless communication system 10 and an encryption code) and (page 2, paragraph 24, receiving the signal transmitted from the wireless communication system; extracting the specific number and the encryption code from the received signal).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of receiving the encryption codes of the data processors using the teaching of Kim in order to receives the encryption code in addition to the encrypted data and verify the encryption code.

A code management control portion that compares a plurality of the encryption codes received by the code management reception portion; and a result output portion that outputs a comparison result yielded by the code management control portion, (abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose the system of comparing the received encryption codes. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 23, a receiving unit for receiving the signal transmitted from the wireless communication system; a storage unit for storing a specific information of the wireless communication system and an encryption code; a control unit for determining whether the specific information and a numerical information included in the signal received by the receiving unit are consistent with the specific information and the encryption code stored in the storage unit; a security setup unit for setting up and canceling the security status in accordance with the results of the control unit; and a setup key for storing the specific information and the encryption code of the wireless communication system to the storage unit and setting up operation of the control unit) and (page 3, paragraph 52, as described above, the security system according to the present invention is implemented by using the specific information of the wireless communication terminal, the encryption codes which is up to infinity).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of comparing the received encryption codes using the teaching of Kim in order to identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Wherein the data processors include a code management transmission portion that transmits the encryption codes of the data processors themselves to the electronic apparatus.

Art Unit: 2439

(Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

Son does not explicitly disclose the system of transmitting the encryption codes of the data processors to the electronic apparatus. However, in the same field of endeavor, Kim teaches this limitation as, (page 1, paragraph 2, the present invention relates to a security system using a signal transmitted from a wireless communication terminal and a security method using the same, and more specifically to a security system using a signal transmitted from a wireless communication terminal).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of transmitting the encryption codes of the data processor to the electronic apparatus using the teaching of Kim in order to substitute one method for the other to achieve the same end result of transmitting encrypted program (encryption code) from data processors (wireless communication terminal) to electronic apparatus (security device).

Claims 21, 26, 38 and 39 are rejected under the same reason set forth in rejection of claim 1:

As per claim 2 Son in view Kim discloses:

The encryption code management system of claim 1, wherein the data processors include an encryption portion that encrypts a signal transmitted from the code management transmission portion to the electronic apparatus. (Page 3, paragraph 39, first, a video program is encrypted by video on-demand source, then the encrypted program is transported to a remote server via network).

As per claim 3 Son in view Kim discloses:

The encryption code management system of claim 2, wherein the electronic apparatus includes a decryption portion that decrypts the signal received by the code management reception portion from the data processors. (Page 3-4, paragraph 34, the video program, encrypted by video on-demand source and transported to remote server, decrypted by the remote server using the first key).

As per claim 4 Son in view Kim discloses:

The encryption code management system of claim 2, wherein an encryption key to be used to encrypt the encryption codes is transmitted from a side that receives the encryption codes and the comparison result. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

As per claim 5 Son in view Kim discloses:

The encryption code management system of claim 4, wherein the encryption key used for encryption in the data processors is transmitted along with a code request signal transmitted by the electronic apparatus to request the data processors to transmit the encryption codes. (Page 3, paragraph 40, the private key(s) itself may be transmitted from the source to the server while encrypted in a second encrypted form or communication channel which is separate from the communication channel).

As per claim 6 Son in view Kim discloses:

The encryption code management system of claim 2, wherein an encryption key having been used to encrypt the encryption codes is transmitted, along with the encryption codes and the comparison result, from a side that transmits the encryption codes. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

As per claim 7 Son in view Kim discloses:

The encryption code management system of claim 1, wherein the electronic apparatus includes a code storage portion that stores one or a plurality of the encryption codes received, (page 2, paragraph 28, after the encrypted program is transported to the remote server, the remote server stored the encrypted video). Also see fig. 5A block 506.

Wherein the electronic apparatus first receives, via the code management reception portion, the encryption codes from the data processors and then stores the received encryption codes in the code storage portion, (page 2, paragraph 28, after the encrypted program is transported to the remote server, the remote server stored the encrypted video). Also see fig. 5A block 506.

Then receives, via the code management reception portion, the encryption codes from the data processors other than those corresponding to the encryption codes stored in the code storage portion, (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by the source and the encrypted program is then transported to the remote server) and (page 1, paragraph 20, the cable network typically includes one or more broadcast sources, one or more premium broadcast sources and also video on-demand). Since the cable provider has different broadcast sources, the remote server can accept different encrypted message and store them.

Then compares, in the code management control portion, the encryption codes received by the code management reception portion with the encryption codes stored in the code storage portion to search for coincidence, and then yields a search result as the comparison result. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose the system of comparing the received encryption codes. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 24, receiving the signal transmitted from the wireless communication system; extracting the specific number and the encryption code from the received signal; comparing the extracted information and the extracted encryption code with the specific information and the encryption code stored in

Art Unit: 2439

the storage unit; and setting up or canceling the security status by operating a security setup unit when the results are consist in the comparing step).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of comparing the received encryption codes using the teaching of Kim in order to identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Claims 15 and 16 are rejected under the same reason set forth in rejection of claim 7:

As per claim 11 Son in view Kim discloses:

The encryption code management system of claim 7, wherein the electronic apparatus includes, one for each of the data processors with which the electronic apparatus has communicated, registration keys with which to register identification codes by which the data processors are identified, and wherein the electronic apparatus stores in the code storage portion the encryption codes along with the identification codes registered with the registration keys. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

Son does not explicitly disclose the system having an identification code that identifies the data processors. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 24, the security method using a signal transmitted from a wireless communication terminal according to the present invention, comprises the steps of: inputting the specific number of the wireless communication terminal of a certified user and an encryption code set by a user).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of having an identification codes that identifies the data processors using the teaching of Kim in order to

Art Unit: 2439

identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Claim 31 is rejected under the same reason set forth in rejection of claim 11:

As per claim 12 Son in view Kim discloses:

The encryption code management system of claim 11, wherein, in the result output portion of the electronic apparatus or the data processors, the communication systems composed of a plurality of the data processors among which the encryption codes are coincident are indicated by displaying the identification codes thereof to indicate groups to which the plurality of data processors belong. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

Son does not explicitly disclose the system having an identification code that identifies the data processors. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 24, the security method using a signal transmitted from a wireless communication terminal according to the present invention, comprises the steps of: inputting the specific number of the wireless communication terminal of a certified user and an encryption code set by a user).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of having an identification codes that identifies the data processors using the teaching of Kim in order to identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Claim 32 is rejected under the same reason set forth in rejection of claim 12:

Art Unit: 2439

As per claim 13 Son in view Kim discloses:

The encryption code management system of claim 11, wherein the identification codes are installation positions and types of the data processors. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose the system having an identification code that identifies the data processors. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 24, the security method using a signal transmitted from a wireless communication terminal according to the present invention, comprises the steps of: inputting the specific number of the wireless communication terminal of a certified user and an encryption code set by a user).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of having an identification codes that identifies the data processors using the teaching of Kim in order to identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Claim 33 is rejected under the same reason set forth in rejection of claim 13:

As per claim 14 Son in view Kim discloses:

The encryption code management system of claim 11, wherein the identification codes are device names of the data processors. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose the system having an identification code that identifies the data processors. However, in the same field of endeavor, Kim teaches this limitation as, (page 2, paragraph 24, the security method using a signal transmitted from a wireless communication terminal according to the present invention, comprises the steps of: inputting the specific number of the wireless communication terminal of a certified user and an encryption code set by a user).

Art Unit: 2439

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the system of having an identification codes that identifies the data processors using the teaching of Kim in order to identify the incoming signal (code) and verify the signal received to setting up or canceling the security status using the security setup unit.

Claims 18, 34 and 35 are rejected under the same reason set forth in rejection of claim 14:

As per claim 17 Son in view Kim discloses:

The encryption code management system of claim 1, wherein, in the result output portion of the data processors or the electronic apparatus, a plurality of the data processors among which the encryption codes are coincident and that thus build one communication system are displayed as one group. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

Claim 30 is rejected under the same reason set forth in rejection of claim 17:

As per claim 19 Son in view Kim discloses:

The encryption code management system of claim 1, wherein the electronic apparatus is a remote control unit for operating the data processors. (Page 2, paragraph 34, the encrypted program is transported via a primary distribution network from the video on-demand source to a remote server within a distribution center).

Claim 36 is rejected under the same reason set forth in rejection of claim 19:

As per claim 20 Son in view Kim discloses:

The encryption code management system of claim 1, wherein the data exchanged between the data processors is AV data. (Page 1, paragraph 3, the present invention relates to the field of video distribution networks in particular, this invention relates to secure video distribution networks).

Claim 37 is rejected under the same reason set forth in rejection of claim 20:

As per claim 22 Son in view Kim discloses:

The encryption code management system of claim 21, wherein the data processors include: an encryption portion that encrypts a signal to be transmitted from the code management transmission portion to the electronic apparatus; (Page 3, paragraph 39, first, a video program is encrypted by video on-demand source, then the encrypted program is transported to a remote server via network).

A decryption portion that decrypts a signal having received by the code management reception portion from the electronic apparatus, (page 2, paragraph 32, At the subscriber stations 110, the multiplexed signal is demultiplexed to isolate the re-encrypted program in the second encrypted form, the re-encrypted program is decrypted from the second encrypted form to generate the unencrypted video program, and then the video program is displayed).

Wherein the electronic apparatus includes: an encryption portion that encrypts a signal to be transmitted from the code management transmission portion to the data processors; (page 2, paragraph 31, after the video program is re-encrypted, the re-encrypted program in the second encrypted form is multiplexed with other signals to generate a multiplexed signal. The multiplexed signal is then distributed 516 via the secondary distribution network to the subscriber stations).

A decryption portion that decrypts a signal having received by the code management reception portion from the data processors. (Page 3, paragraph 34, the remote server decrypts the video program from the first encrypted form).

As per claim 23 Son in view Kim discloses:

The encryption code management system of claim 22, wherein an encryption key to be used to encrypt the encryption codes is transmitted from a side that receives the encryption codes and the comparison result. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

As per claim 24 Son in view Kim discloses:

The encryption code management system of claim 23, wherein the encryption key used for encryption in the data processors is transmitted along with a code request signal transmitted by the electronic apparatus to request the data processors to transmit the encryption codes. (Page 3, paragraph 40, the private key(s) itself may be transmitted from the source to the server while encrypted in a second encrypted form or communication channel which is separate from the communication channel).

As per claim 25 Son in view Kim discloses:

The encryption code management system of claim 22, wherein an encryption key having been used to encrypt the encryption codes is transmitted, along with the encryption codes and the comparison result, from a side that transmits the encryption codes. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

8. Claims 8-10, 27-29 and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al (Son) (US Pub. No. 2001/0017920) in view of Kim (US Pub. No. 2003/0164750) and further in view of Garfinkle (US 5,400,402).

As per claim 8 Son in view Kim discloses:

The encryption code management system of claim 7, wherein, when the electronic apparatus recognizes that a predetermined period of time has passed after the encryption codes were stored in the code storage portion, the electronic apparatus erases the encryption codes from the code storage portion. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son in view of Kim does not explicitly disclose the system of erasing the encryption codes from the storage after a predetermined period of time has passed. However, in the same field of endeavor, Garfinkle teaches this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and Kim to include the system of erasing the encryption codes from the storage after a predetermined period of time has passed using the teaching of Garfinkle in order to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

Claim 27 is rejected under the same reason set forth in rejection of claim 8:

As per claim 9 Son in view Kim discloses:

The encryption code management system of claim 7, wherein, when the electronic apparatus recognizes that coincidence with the encryption codes stored in the code storage portion has been found more than a predetermined number of times, the electronic apparatus erases the encryption codes from the code storage portion. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

Son in view of Kim does not explicitly disclose the system of erasing the encryption codes from the storage after a predetermined period of time has passed. However, in the same field of

Art Unit: 2439

endeavor, Garfinkle teaches this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and Kim to include the system of erasing the encryption codes from the storage after a predetermined period of time has passed using the teaching of Garfinkle in order to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

Claim 28 is rejected under the same reason set forth in rejection of claim 9:

As per claim 10 Son in view Kim discloses:

The encryption code management system of claim 7, wherein the electronic apparatus includes an erasure operation portion that erases from the code storage portion the encryption codes stored therein. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son in view of Kim does not explicitly disclose the system of erasing the encryption codes from the storage area. However, in the same field of endeavor, Garfinkle teaches this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and Kim to include the system of erasing the encryption codes from the storage area using the teaching of Garfinkle in order to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

Art Unit: 2439

Claim 29 is rejected under the same reason set forth in rejection of claim 10:

As per claim 40 Son in view Kim discloses:

The encryption code management system of claim 1, wherein the electronic apparatus includes a display portion that display the comparison result. (Page 2, paragraph 22, at the subscriber stations 110, the multiplexed signal is demultiplexed 208 to isolate the video signal, and then the video signal is displayed 210, typically, on a television monitor).

Son in view of Kim does not explicitly disclose the system of displaying the comparison result. However, in the same field of endeavor, Garfinkle teaches this limitation as, (column 4, line 19-24, the order data may be also inputted to the comparator 36 and compared to order data also encoded in the down-loaded data from the central station. If there is an error between the order data inputted from order unit 24 and the down-loaded order data, an error detector 46 can provide an input to microprocessor 30 to display an error message on television screen 18 and, if desired, block the storage of the video data.).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and Kim in order to substitute one method for the other to achieve the same end result of displaying information in the device.

Claim 41 is rejected under the same reason set forth in rejection of claim 40:

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

Art Unit: 2439

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

January 15, 2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434